МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО- ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №3

Варіант 2

з дисципліни

Криптографія

З теми: « Криптоаналіз афінної біграмної підстановки »

Перевірила:

Селюх П.В

Виконав студент групи ФБ-92

Андрієвич Дмитро Юрійович

Мета роботи: Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Завдання:

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.
2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).
3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи (1).
4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Код програми знаходиться у файлах **main.py** та **text_processing.py**.

Хід роботи: спочатку я створив функцію, яка обчислює обернений елемент за модулем з використанням розширеного алгоритму Евкліда. Потім я створив функцію, яка вирішує лінійні порівняння, також я передбачив випадок коли лінійне порівняння має декілька розв'язків. Далі за допомогою алгоритму, реалізованого у ході першої лабораторної, було знайдено 5 найчастіших біграм. Далі був створений алгоритм, який зробить всі можливі пари з двох списків по 5 елементів (без діагональних пар). Для кожної пари було розв'язане лінійне порівняння та знайдені можливі ключі a та b. Після цього кожним ключем було дешифровано шифртекст та за допомогою критерію частих біграм було знайдено єдиний змістовний текст.

Результати:

П'ять найчастіших біграм шифртексту:

```
The most frequent bigrams in cipher text: ['йа', 'юа', 'чш', 'рп', 'юд']
```

Розпізнавач російської мови реалізований з використанням критерію частих біграм. Якщо частота будь-якої біграми з найбільш поширених у російській мові менша за певне значення (знаходилось з результатів першої лабораторної роботи), то цей текст відкидається.

Шифрований текст, варіант 2:

рйрщкагппрфчгшрщйрпрффькрпьчшдвиыеюдучхулицплшюшашдщныскюшвпьюкджьйах
ещыйеьеюоэдсецчтыкйдшщчзюимевжшбушччэканылшолшкюшчшэизупмзсбвжшбуойшаи
щмдпнрйуюфшхдтылшларюдезанпрбкажлащваэщюемечшщипнипнучбусхекайаэкяуклзщ
югхегарпинцплппрффзшскыушшммеючогалчцпдшяуыуйацднфзхащаукйнхжукчщысаэар
южштнцмосхрхлтечшишваллмппртелиюдьпкуурдшерритыачтахщышкаюйзхцмздффнаге
щцлерьюбокцезацчучрйяыыунлсрорпрькрщэарючолаимхугшзепутэрщбероюазанхзушщим
зсбючолаштэиэщюхжукчтдюагпшдормэрмыупьфуйабеюемдвитылшошрщышгпфуыуйацд
аюваллйыачларщзшроюалахдорцпиыщылшошрщйьфуйазлиекдвифущлбшашваллюсхщро
хеццэирщэаэшуоьюдэисфуриыугшэпзлиекдкглаедюднфэщйдшгфчпрбердрйуюпнсабдпннх
цмрцсдрпющкммылеешбпымюенпчшроюабучштечшюдушлсбубеюыхрдщндщфщейерйсдк
ммьофкаюйажйаидхйьнхерщхлкшьсжуиеишбпымюенпчшроюаеймюбероюарпинымжизар
опйхлбшбуклзщзсэпюаиечшорэпьчкгипгекбхщжачойатеашваюдюдкйчбйкпмтырйюенщлу
чихечшчрпрфуклзщрусипнрйыуйаусйрпнцмшяхукчкйбвжшлжпшюечукемипнипцчушлсрй
хпэснезщжмюдкенлхарпсдхйьчмэешйарпхппрэщцжыщпаюехдпьхуйанацчрбюдхушчкацкд
щтеэдвиййтагшфичиорхлфдщфкшышвамносвиййдзьрыщышхемсующудршджьюанхрэцпы
мздффнарписюахьхууочрфчгшйкпаюехдсджжгшцчтыкйдшнануэифуларизсййушфиюдюда
юышькющяпцлдчьншгашэлашьухаедвизлиекдвидщлсхпкеышйрьчценавсачэаькудбюяхцм
рцсдрпгекммылекдхйыуыщйаудюлцчисуюэиффриещжзьргшкдыууоьдглэшешбероюачпщы
лшышдшэасуйаьпымкуюсщгхелафитбюазуыщюаешуоналаолфдыууозмсдщьбукаощжзьры
щаыпмяызшхпбьйацчзюимпелумсрйюасавдыугшбрмэтдйкяуришпчиоскчтхэейыосййричи
кзддрятарщроюазахачшфщчшурпрбуашькщепщчшфитдьчфщроюазацквснхтбьечшчыачеш
удкгхавклаяхбмхашнэпосюеюазнтдщьбудшщепщчшфикайаэкишныцмбээелучылшрщашо
шзсбужифчмэйкблкмоснфэщкылшрщхлиечшритэзалаеймюбероюарптылшцюцрчийщпаюе
ющчшхпэщхеишашйамущьбукаьэзхцмустдмшыщдшцчсдхйыуышйаудчикабпсаюезлиекдф
фыршдчимшлчлэфуюаззддрятачшсающчшййнцусюаьжхезнмшйщгпридщнйымюдкебдкй
ющешхщнкшлнуюсэебдьебпщьюарпжиегтдлэфщюенщдезаламдосусжулапасйюдаюнежсщ
ьйкэытэшсосгпэпщепщчшфихехщюедшэпеемучщройкэысарепуосхасасйленкссвссеоамдос
впхрзшмейрцлтедчусхеццкемчььсдмэшсрморушнллирмффаыпмяызшщфзсййымзсхажала
фщнпбупюоьюдкеещхщшпщяавцквснхтбьечшджпшюешпщьбуказаэплахщдщнйдщгечшд
жпшюешпщьбуэщшчсщряаюэщкацкышщехеаитбюарщлсцпэсеегпосщерпусдюйаюдбучих
еэдэппртехарпеылегшмчхухаяютечшюдуссайщсллдыууокайасазаопчичпнхбморешэшсаю
щуонафщгшмейррихушкдщнйдщгечшщукайаэкышхемчтэхевателуцчисхпкучызшцшмейр
яжпшюешпщьбудшоылшишщгамуыщюаешлуьпрринхдщцадуришпчичифубелшмшмвкйуы
гшхлвпьюзсййушфиюдпелучырйнхюайажлэщцжйацчушугрйхпцчсдьчфщроюаепжьюдмш
еемучщроюазацчаябуашыщдшварчмэчинкныцмйквыдщлагчмэашзщэиьчщцчшмейртвещ
жзьргшкдтваыпмяызшыыдщнпщьбукачэрщмечшлжйазакмхйтвдебукчкйбвжшоыачлаоыьч
мбюдпаюехдхввамнхукчкйбвжшгсйасандуссагшяснежсчикммылезлиекдбюфшхдиырйгекб
юдтдфчнцюдавлэкдусосйасадуклзщюдфчнцюдкемсуювпьюцкдщгечшэиашваейнцусюазбл
эчшгечофщгесаьпюачпжжпшюечуаюгарпсенуказаэпюазшлууросйасажлешзлйаудрйхрмэц
пфжйахеродюыщжрпроппрчикммылевлщднхбмнхшсзмгьхпэсрежаолфдыууофнрйнцусюаз
блэчшрщзщжацчтыкйкаешхакмхйтвжшусййушфиюдюдаюгпшгцчтыкйкающамджйазаддх
ухегарпцпбьюахщэдкгщыфутдаюащышэылшищяросчшмезахехщяпвсхйюдаюыущаидвцю
даюьичбзлцчтыкйэщышты аччбзстдаюышхехаедюшзщрпщысагшлайеощкнуфносачзюид
цецчхйхажатечшжьйацчтыкйдшрщзщашчоыйыуйаусйрпнюлтевйвпрпгечпщачшкдььрмег
фчпрбелшщающашчопаюебушщькышзшвыйафщышхпцмдрщыыуюехакчщуиезафнщыачч
бзстдаюрщлаеебдкйлщйачнрйюблэчшшхнфрпющэплщцчсдфмчзьчжлаыпмяызшжхбмнхш
сбужичлщерпюабуашькщыдшвйрмыулпбьйашдтыцмюарпхвцчьрдшгшашчоламчэичаэхшс

тдаюриэщйазнзсзшйшлшюагпчиеысагшлайезщайхлбшглэщйщчшчамеешвдбювсрэжичбзл
эпрешхнфрплацсрчцпхюшрфчсимэоскгфуыйыхффэплщгарпсенуказарчыупмхуэсдммэтдяа
вдчишхтаичшзыйыуйаусйрпнушхакмюбпмншжлэщйщчшэирщлэгерпюабуосйещеэдсечуш
гцмпнщьбукаюдуыдщимюдкечушгмшрщашщппрэщкырйдщылщеюшвпьюриюдюашдйржа
хетсййвпэсгпчинаькгшхпннзщццтвкчисжлзсйепртшййыуйаусйрпншдажйазмгьусффшлшр
безахемчтэлекмаюрщудеапамдосшсцпфжнлзуышюазреызшэатдрмхпщьбудшщыхубвчочп
щаэщялчохехалюидвиаммсееапегкажлхехдпрчиилмечшшшщкдщтечшчызшэатдрмлэчлрщ
наэшэдкйчбйкишугрййкоыдднпрщышлсбубеаунккмнежскгцчтыкйкавйыуйаусйрпносфнзв
юаиейркезаокйщгаынрйщызюимюдаюаыпмяызшцлгпшгцчтыкйкаяхбмщырйнхкелиачгшш
дсдмэшсрмфукукчщгчилиачгшзсечмбрмфуэснарпзючшпмвпфчбшмейрпныурщгпзхцмчэи
орщэаэшшщрщхезакдььрмьрпнхщшдькюедефщроошкаюрпркдчэуырщлхчээпмеидбюхахщ
имюдюарппьщсрплаэщкаюытэтедщпуэщвкющиулаэиыйхллланажахоусиппрсеэщюхыййаьк
эиеыйееуйафмыущфзщжбглщейеуозсащвашйымюдхунлищжанарпзючшбуосачиеэдщырйн
хюахйщфрпешбероюарущефпкезарчцптддчщфдщпуэщвкющньйашегахлтейицмрйыезаокн
ейежпэиэщгэхувлуоыуыщимфмйщпшйрщьйапахпьююаяофэхувлуолиачйахагаодвимдчит
ысазшйыжжйажлчпнхыезахаэасачшашйарокамейецыьпяйхеейыуйаусйрнфйщхлюеерффас
хйюдкемдсилэгерпйклижуашрщщейечшвппршгцчтыкйканущефптачшгэрщзщяпэптбьерпи
мюдкеслщешцримежагекаюрэпьчяфьеруюсхпымздюлщелшашфьымосьрчифшцкщедеюака
йасажлнктешщэилиачгшопьчффкммьофпаюечэрщошбеюеюылшищгаясбрмэтдюадуклзща
чисюарехеэдпрмэтдавнкхатешщашлиачгшдчьнчиипяыачжижуыщашащышгпридчьнрифус
ицлщеомхпипчушгмшрщашгшмейрсемьюдкеипгекбхщвпчпжжйаайхлзаейуюфшроошэщн
хльюаэпеямшцевлэияффубелшшфцчтыкйхрмсуювпьюышдшварчмэчиащварщэщйщчшэи
йщхатешщчшбущефпсдюдисфуидчиеапячщ

Розшифрований текст, варіант 2. Ключ – a = 27, b = 211

однакоэтакартинаскакойшьстжроньмдеенирассматривалиралчльваетйявнлптонеичреьелен
ноепрвчадкипроявляющиесярезколчрикусьваниемусиливающиесядоопасногодляжизнвчри
водящегоктяжкомусамокалечениюмогутвсежевнекоторьхслучаяхнедостигатытакойсильцс
лабляясыдократкихсцстоянийабсансадобьстричроходящихголовокруженийимогуттакжесм
енцтысякраткимвчериодафикогдаболыной совершаешпуждьеегоприродячцступкикакшьна
ходясывовластибессознателыногообуславливаясывобщемкакбьстранноэтониказалцсбпист
отелесньмвчричинафиэтисцстояниямогумчервоначалыновозникатфчичричинатпистодуше
вньмиспугилимогутвдалынейшемнаходитыйявзависимцстиотдушевньхволненийкакнихар
актернодляогромногоболышинствацлщпаевинтнллектуалыноеснижениеноизвестезчокрай
неймереодинслщпайкогдаэтотнедлгненарушигвьсшейинтнллектуалыной деятелыностигнл
ымголыцдругиеслучаивотношениикотжрьхутверждалосытожесамоененадежньилвчодлежа
тсомнениюкакислучайсамогодцстоевскоголицастрадающиеэпилепсиеймогутпроизводиты
впечатлениетупостинеджразвитоститкакакэыаболезнбпастосопряженасярковьраженньмид
иотизмомикрупнейшифимозговьмидефэкыафинеявляясыконлпнообязатнлыной составнопп
астыюкартиньболезниноэтипрвчадкисовсемисвоимивидоизмененияфишьваютиудрлгихли
цулиосполньмдушевньмразвитиефискжреесосверхошьчнаявболышинствеслщпаевнедцсыа
точноуправляемойимиаффэктивнцстыхнеудивителыночтичриыакихобстоцтнлыствахневоз
можноусыановитысовокупнцстыклинопескоюаффэкыацчилячсиитфптопроявляетсяводнор
однцстиуказанньхсимптомовтребуемчовидимомуфункционалыногопониманиякакеслишь
механизманжрмалыноговьсвобожьенишчервичньхпозьвовбьлподготовленорганопескимех
анизмкоторьйилчолызуетсшчриналичииивесымаразньхусловийкадчринарушениимозговойд
еятелыностьвчритяжкомзаболеваниитканейилитоксопескодзаболеванииыакипринедцсыато
чномконтроледушевнойекономиикризисномфункционированиидушевнобэнергиизаэтимра

зднлениемнадвавидамьчувствуемньентопностымеханизмалежащеговосновевьсвобождени япервопныпчозьвовэтотмеханизмнедалекиотсексуалыныпчроцессовпорождаемьхвсвоейосн ователоксическиужедревнейшиеврюпиназьваликоитусмалойцчилячсиейивидныливполовомак тесмяйпениеиадаптациювьсвобожьенияэпилептопескогоотводараздраженияэпилептопеска яреакциякаковьфименемможноназватывсеэтовместевзятоенесомненнотакжепостнчаетивр аспоряжениеневрозасущнцстыкотороговтомчтобьликвидироватысоматическимассьраздра женияскоторьфиневрознеможетсправитысшчсихическиэпилептопескигчрипадоксыановит сцтакимобразомсимптомомистериииеюадщчтируетйяивидоизменяетсшчодобнотомукакэт опроисходитпринжрмалыномтлпениисексуалыногопроцессаыакимобразоммьлчолньжчрав омразличаемжрганическуюиаффэктивнуюцчилячсиачрактопескоезначениеэтогоследую ще естрадающигчервогчжраженболезныюмозгастрадающийвторойневротиквпервомслщпаеду шевнаяжизнфчодверженанарушениюизвневовторомслучаенарушениеявляетйявьражением самойдушевнойжизнивесымавероцтночтоэпилепсиядостоевскогоотносится яковторомувиду точнодоказатыэтонелызяыаккаквтакомслщпаенужнобьлобьвклдпитывцелокупнцстыегоду шевнойжизниначалопрвчадковипоследующиевидоизмененияэтихпрвчадковадляэтогоунас недостатфпноданньхичисаниясафипчрипадковничегонедаютсведенияцсоотношениянмежд упрвчадкафивчереживанияфинеполньичастичротиворечивьвсеговероятнеепредположенил птопрвчадкиначалисыьдцстоевскогоужевдетствечтоонивнюпалехарактеризовалисыболеес лашьфисижчтомафиитолыкичцслепотрясшегоегичереживаниянавосемнадцатомгодужизни убийстваотцапринялифжрмуцчилячсиибылобьвесымауместноеслишьичравдалцсытфптоон вчолностыюпрэкратилисывовремяотбьванияимкаторгивсибириноэтомнчротиворечатдруги еуказанияочевиднаясвязымеждуотцеубийствомвбратыяхкарамазовьхисьдгбойотцадостоев скогобрцсиласывглазанеодномубиографьдцстоевскогоипослужилаимуказаниемнаизвестно есовременноепсихологопескоенщчравлениепсихоанализтаккадчодраяумеваетйяименноонс клоненвидетывэтомсошьтиитягчайшуютравмуивреакциидцстоевскогонаэтоклдпевойпунк тегоневрозаеслияначнуобосновьватыэтуусыановкнчсихоаналитопескиичасаюсычтоокажус ынепонятньмдлявсехтехкомунезнакомьучениеивьраженишчсихоанализаунасодиннадежнь йисходныгчунктнафизвестенсмьслпервьхпрвчадковдцстоевскоговегоюношескиегодьзадоу годичоявлениящчилячсииуэтихпрвчадковбьличодобиесмертиониназьвалисыстрахомсмерт иивьражалисывсостояниилетаргическогцснаэтаболезныназодилананеговнюпалэкогдаонш ьлещемалычикомкаквнезщчнаябезотчетнаяподавленностбпувствокакозчозжерассказьвалс воемьдругусоловыевутакоекакбьдтошьемнчредстоялцсейчасжеумеретыивсамомдлненасту палосостояниесовершенничодобноедействительнойсмертиегобратандрейрассказьвасптоф едоружевмолоддегодьпередтемкакзаснутыцсыавлялзапископтобоитйяночыюзаснутысмерт оподобньмсномвчросимчоэтомучтобдегопохоронилитолыкочеребчцтыднейдцстоевскийза рулеткойвведениеснамизвестньсмьслинамерениетакихпрвчадковсмертиониозначаютотож ьествлениесумершимчеловекомкотжрьйьействитнлыноумериличпнловэкомживьмещеноко торомумьжелаемсмертивтжройслщпайболеезначителезчрипадоквуказанномслучаеравноце ненназаниюмыпожелалисмертидрлгомутячерымьсыалисафиэтимдрлгимисамиумерлитут психоаналитическоещпениеутверждаетчтоэтотдругойдлямалычикаобвпноотецииименуемь йистериейпрвчадокявляетйяыакимобразомсамонаказаниемзапожеланиесмертиненавистно муотцуа

Висновки: під час виконання даної лабораторної роботи я засвоїв методи частотного криптоаналізу та здобув навички розкриття моноалфавітної підстановки. Також, я ознайомився з прийомами роботи в модулярній арифметиці.